MATLAB EXPO 2019 Bern

KYBURZ

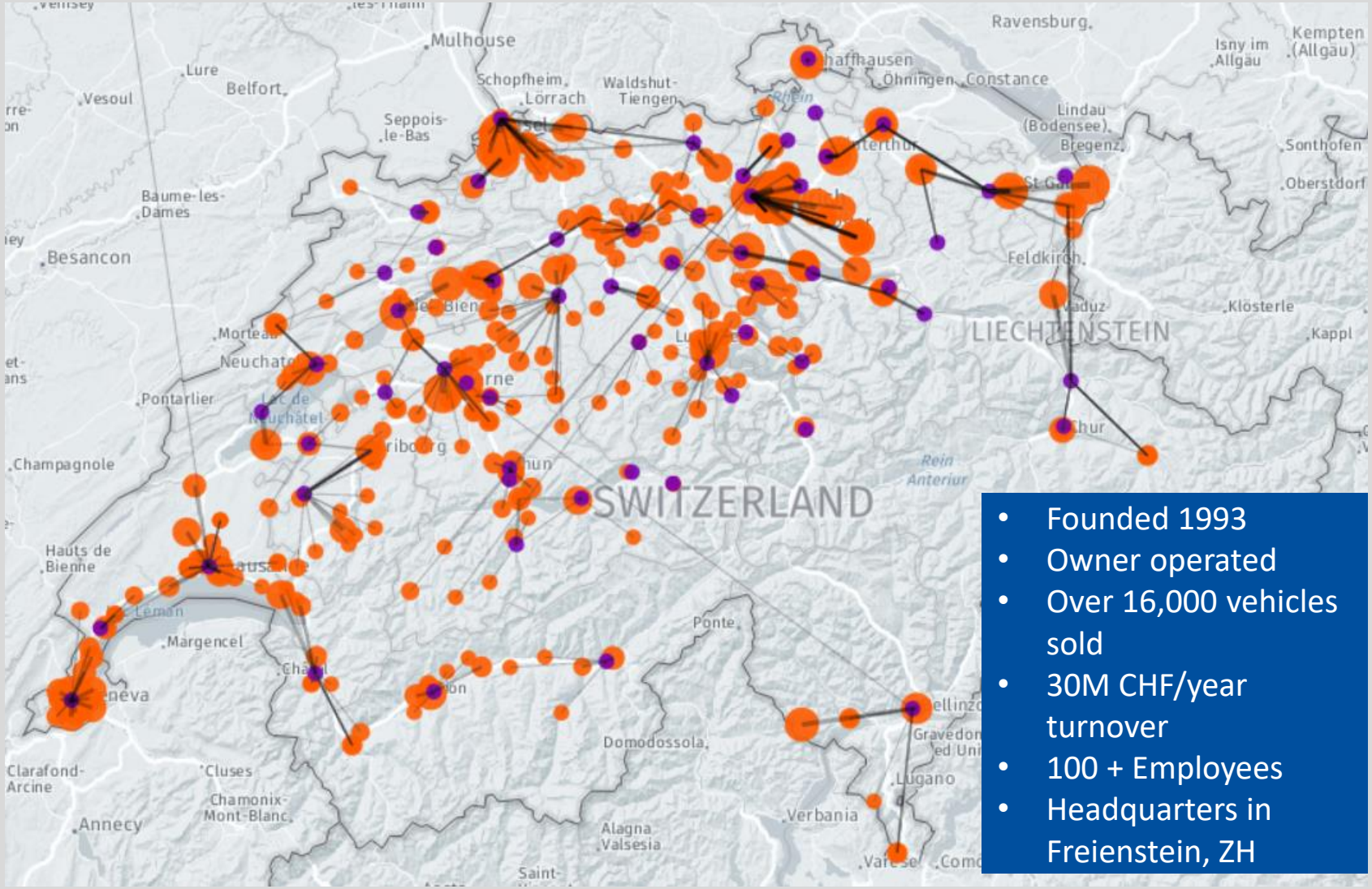
Courtesy of ETH-Zurich, ARC

Designing and controlling safe self-driving systems

Dr. Erik Wilhelm
Head of Research
KYBURZ Switzerland

23rd May, 2019

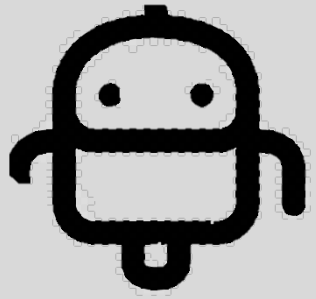
A well-established brand

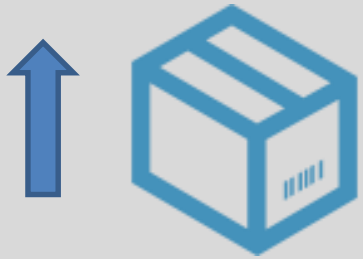


- Founded 1993
- Owner operated
- Over 16,000 vehicles sold
- 30M CHF/year turnover
- 100 + Employees
- Headquarters in Freienstein, ZH

KYBURZ

Changing postal delivery landscape





- Must be:
  - Cheaper
  - Faster
  - More reliable
  - ... More personal?

Prototype series

- Mobile depot box (eT2)
- Sensors
  - 2D Lidar
  - Ultrasonic
  - 360 camera
  - GPS
  - Bump-stop

- Autonomous delivery agent (eT3)
- Sensors
  - 3D Lidar
  - Ultrasonic
  - Infraded
  - INS
  - Bump-stop

- Flexible delivery system (eT4)
- Sensors
  - 3D Lidar (2x)
  - Ultrasonic (8x)
  - Infrared (8x)
  - Radar (4x)
  - GPS (INS)
  - 360 Cameras (localization)
  - 360 Cameras (comprehension)
  - Time-of-flight camera
  - Bump-stop

KYBURZ

Autonomous System Design Challenges

High availability

Image: ABC news

Ap(proved) safety

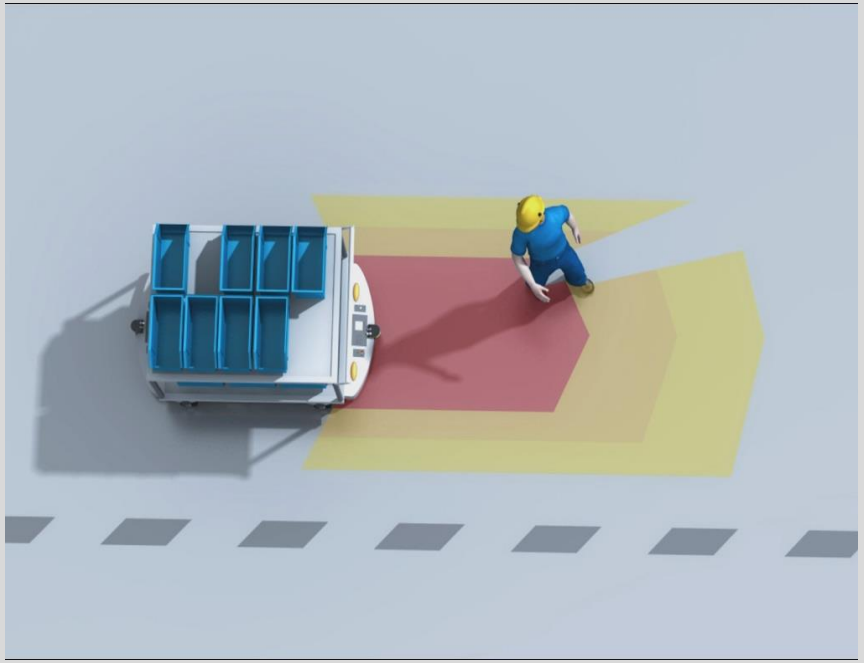


Image: sick.com

Test coverage

Image: youtube.com

Availability Requirement

Image: Frugal Entrepreneur

- 300 parcels/day
- 8.25 hr/day
- 56 kCHF/year

- 40 parcels/day
- 24 hr/day
- 50 kCHF purchase

Image: cnbc.com

- 1 disengagement/day
- 56 hours per year
- 3 kCHF per year

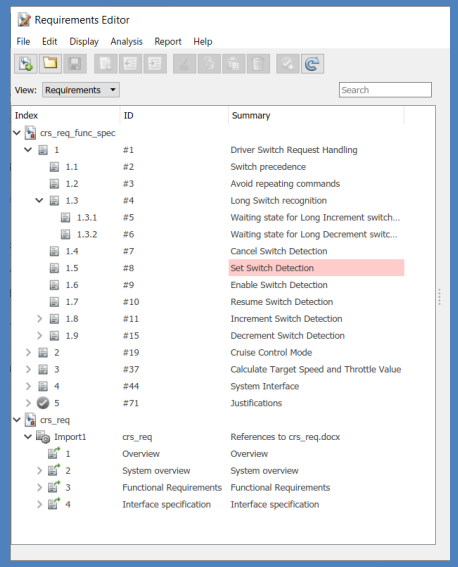
- Robotic delivery amortized with 1 disengagement/day, never with 3 disengagements/day

Sensor and controller redundancy

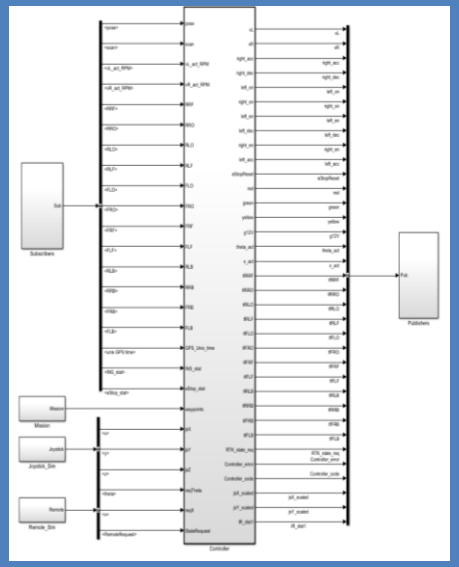
Localization	Day	Night	Precipitation	Fog	Tall structures	Tranparent obstacles	Diffuse obstacles
INS (GPS)	✓	✓	✓	✓	!		
Optical	✓	✗	✗	!	✓		
Pointcloud	✓	✓	!	✗	✓	-	-
Obstacle Avoidance							
LiDAR	✓	✓	!	✗	-	✗	!
Optical	✓	✗	✗	!	-	✓	✓
Radar	✓	✓	!	✓	-	✓	✓
Ultrasonic	✓	✓	✓	✓	-	✓	!
Time-of-Flight	!	✓	!	✗	-	!	✗
Infrared	✗	✓	!	✗	-	✗	✗
Bump Stop	✓	✓	✓	✓	-	✓	✓

Workflow

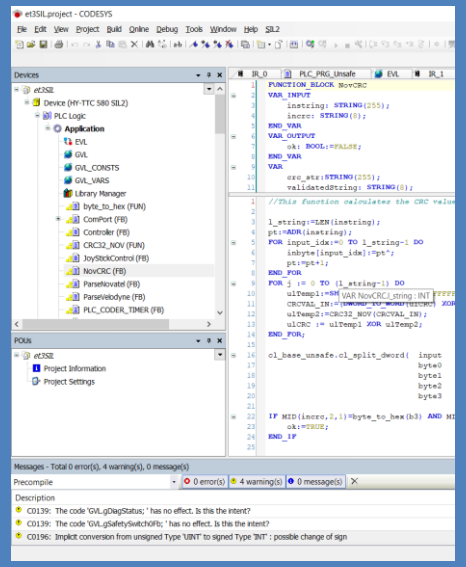
Specifications



Model Based Design



Code Generation

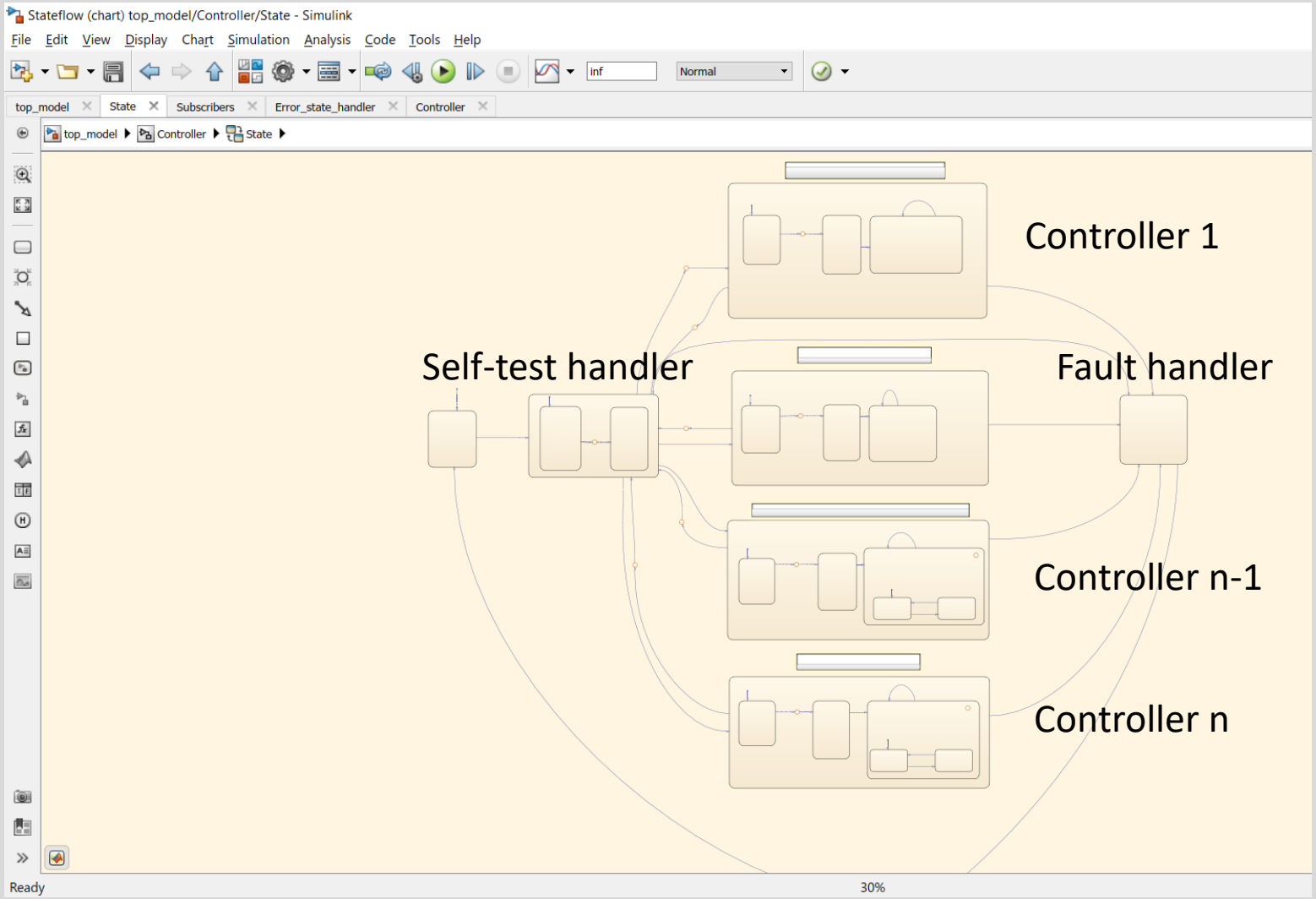


Compilation

- This workflow allows SIL2 certifiable code to be generated using model-based design
- Review and testing occurs within each phase and before each release

KYBURZ

Availability Solution



- Supervisory controller invokes multiple independent and redundant motion control paradigms
  - Local
  - Remote
  - Mission training
  - Mission running
- Graphical state modeling of control logic allows streamlined, debuggable, testable strategies

KYBURZ

Functional Safety and Approvals

- Kyburz is designing autonomous machines not vehicles
  - IEC 61508
- Voluntarily following automotive functional safety norms
  - ISO 13849:2015
  - ISO 26262:2018
- Primary implications
  - Development process
  - Documentation system
  - Component selection
  - Software development toolchains

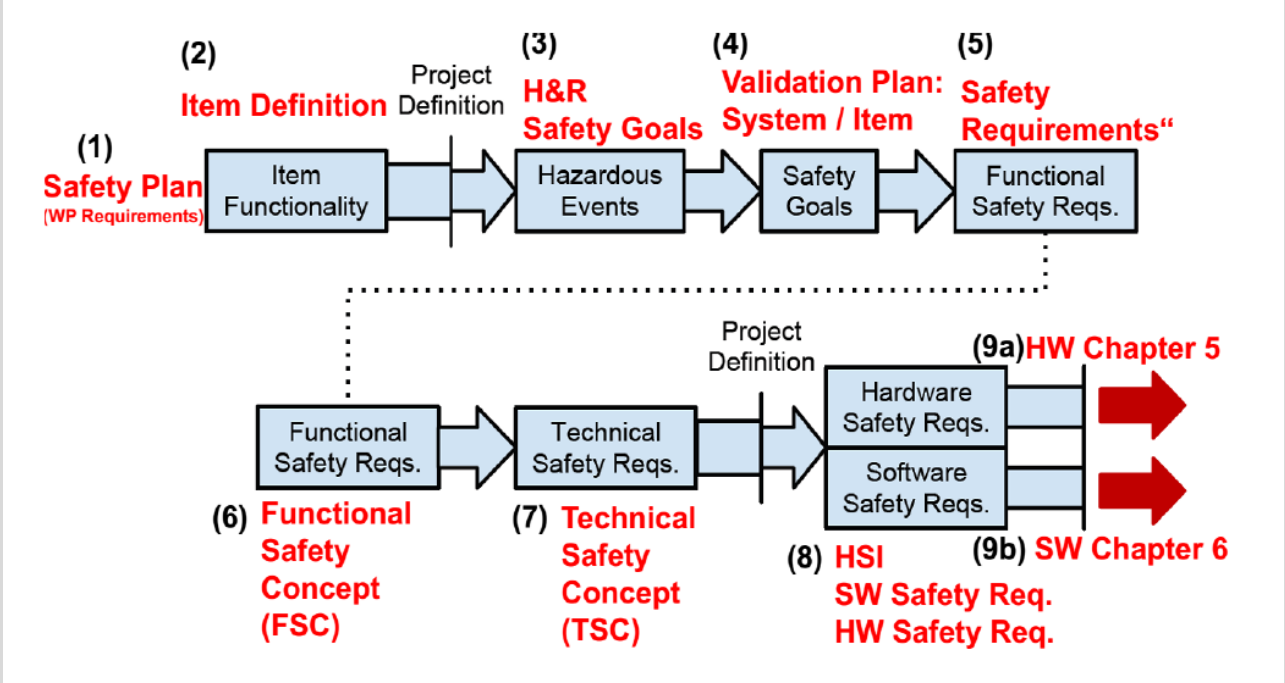
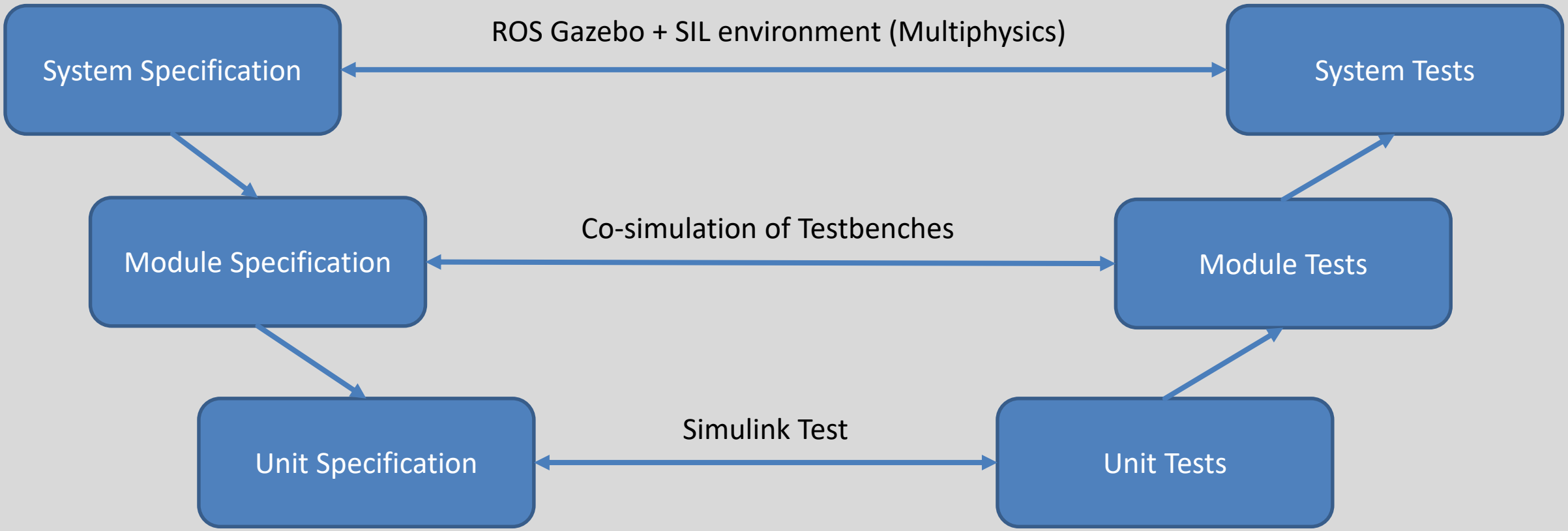


Image: ROSAS Freiburg, Paria Amini

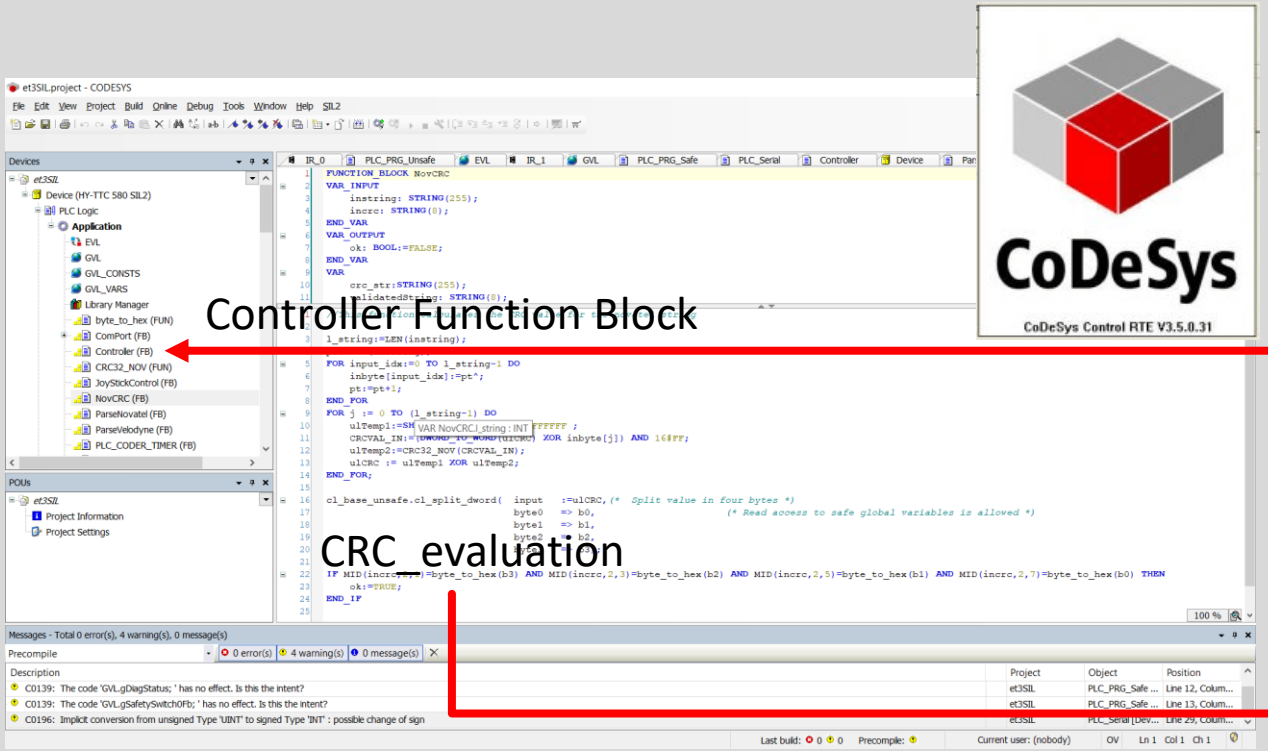
KYBURZ

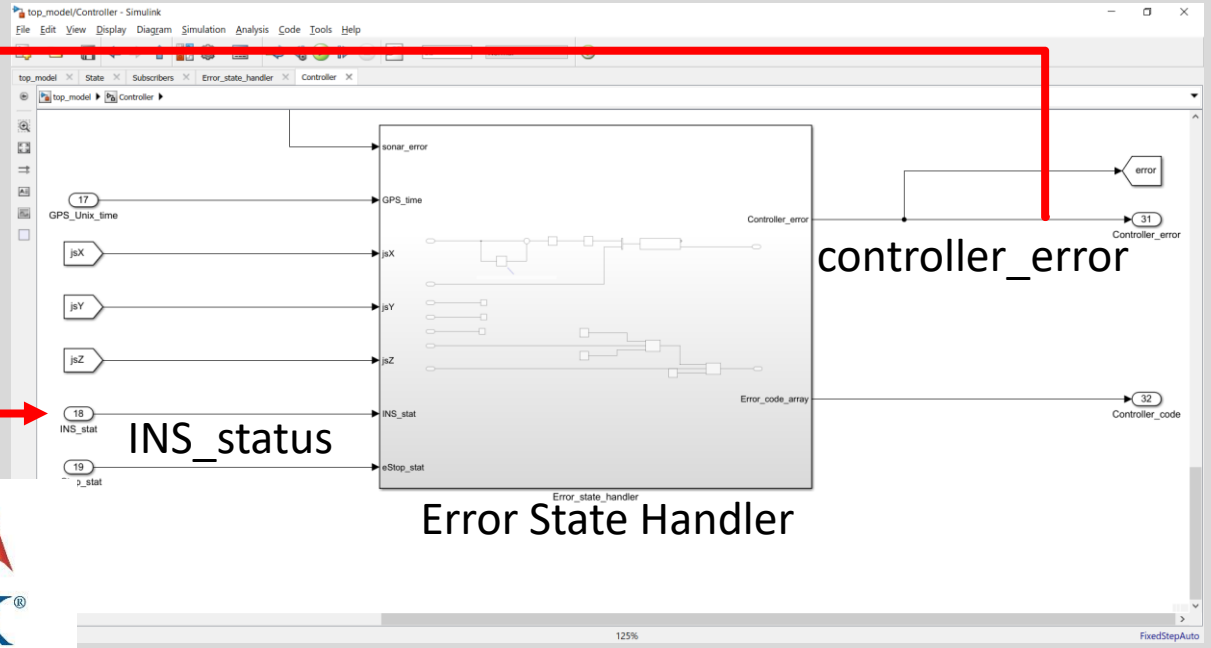
Safety Solution



- Kyburz toolchain uses layered verification techniques and model-based design
- All requirements are easily documented for traceability

Safety Example





- Serial communication errors are detected and handled gracefully in control logic

KYBURZ

Corner Cases

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	S/N	Subsystem	Conditions	Impacted Function	Process Step	Potential Effect	SEV (1= not severe, 10 = very severe)	Potential Causes	OCC (1 = not frequently, 10 = very frequently)	Current Process Controls	DET (1 = very detectable, 10 = impossible to detect)	RPN	Action recommend
2	Risk serial number	Which part of the vehicle is most impacted?	Under which conditions are failures most likely?	Specific aspect of the robot subsystem which is effected	What is the action being attempted?	In which ways can the step go wrong?	How severe is the effect on its surroundings and people?	What can cause the step to go wrong, i.e. how could the failure mode occur?	How frequently is the cause likely to occur?	What are the current controls in place to prevent this occurance?	How probable is the detection of the failure mode or its cause?	Risk priority number RPN = SEV * OCC * DET	What actions can reduce occurance or improve detection?
3	121	Mechanical	near curb navigation	castor lock	driving	road obstruction / edge fall / collision	8		8		8	512	
4			transition in to			move off desired path / navigation fails at dangerous moment (on							
	46	Filters	in	INS drift	navigation	crossing etc)	8		9		7	504	
6	6	Sensors	Sun reflection	Camera	driving	road obstruction / edge fall / collision	10		8		6	480	
7	25	Command center	Unattentive operator	Movement	navigation	move off desired path / navigation fails at dangerous moment (on crossing etc)/collision	8		6		9	432	
8	7	Sensors	Sun reflection	IR/Sonar/Laser	driving	road obstruction / edge fall / collision	8		7		7	392	
9	38	Filters	near buildings	INS drift	navigation	move off desired path / navigation fails at dangerous moment (on crossing etc)	8		7		7	392	
						move off							

Risk (RPN) = Occurrence x Severity x Controllability

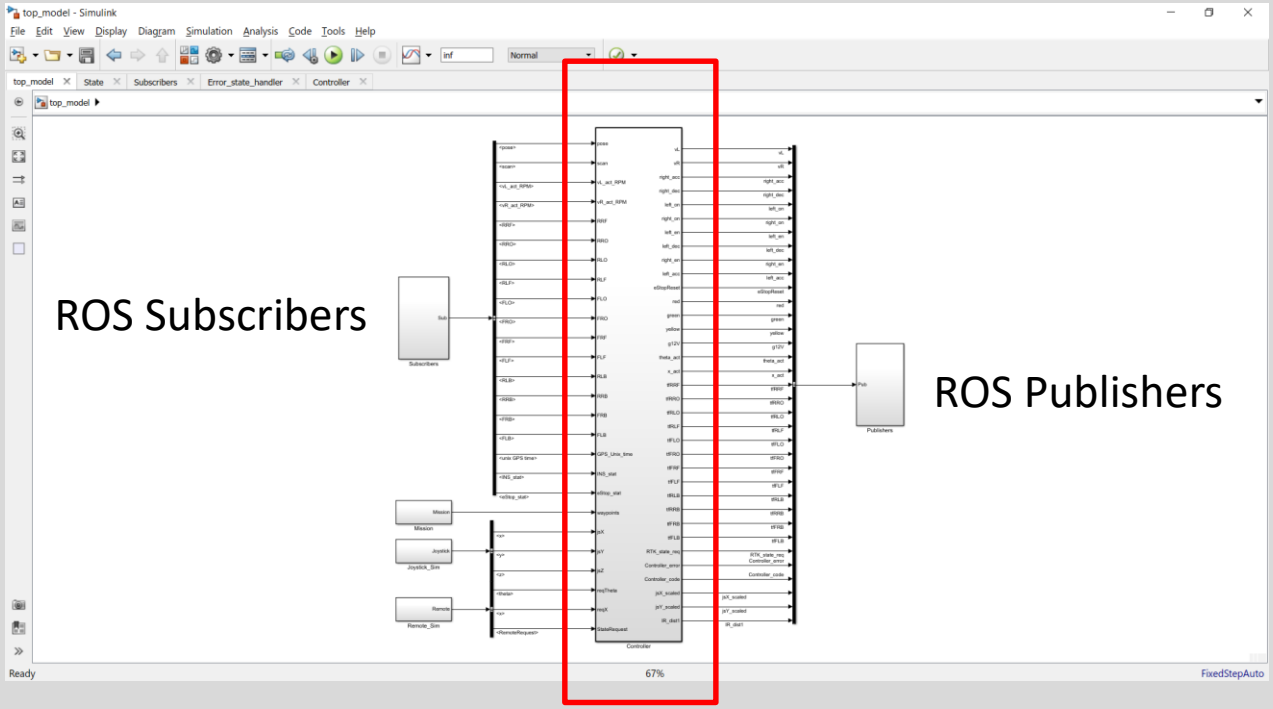
Image: drivingtests.co.nz

Image: arstechnica.com

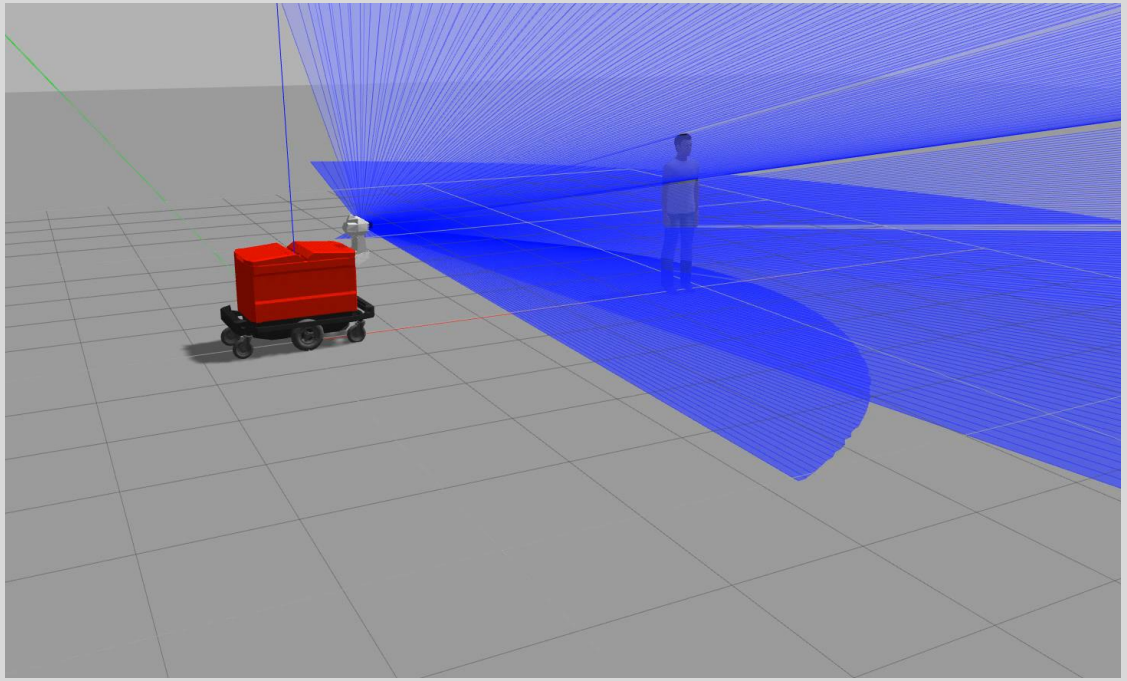
- Hazard and Risk Assessment (HARA) identified 30 failure modes with Risk Priority Number (RPN) > 200, some which are challenging to simulate

KYBURZ

Corner Cases Solution



Autogenerated



- ROS Gazebo enables detailed sensor measurement-level simulation
- With co-simulation testing is drastically streamlined

Corner Cases Example

Summary

- Kyburz Switzerland’s autonomous system developments have saved substantial development time from
  - Enabling seamless and testable control redundancy with finite state machines
  - Integrated toolboxes for streamlining development following functional safety norms
  - Simulation of difficult to test corner-cases with controller to environment interfaces

Thank you for your attention

KYBURZ